Vragen? Opmerkingen? Tips? Mail ze naar brieven@clickx.be.

DOE HET ZELF

Brief van de week

De Clickx-redactie wordt elke dag overstelpt met vragen van lezers. Sommige problemen zijn te specifiek om in het magazine te behandelen, maar andere vragen zijn dan weer zo interessant dat ze meer verdienen dan een kort antwoordje. Daarom selecteren we voor elke Clickx Magazine een vraag van een lezer, die we dan uitwerken in een complete workshop. De vraag vind je op deze pagina, de workshop staat op de volgende twee pagina's. Veel plezier!

(DRAAD)LOOS ALARM!



Mijn draadloze thuisnetwerk is WEP-beveiligd. Je weet echter nooit, en dus zou ik willen controleren wie er via mijn netwerkje aan het surfen is – als het kan graag met een automatische melding zodra er een ongeoorloofde gebruiker opduikt. Hoe pak ik dat aan?

GUIDO EERLINGS



Lezer Eerlings weet blijkbaar de juiste vragen te stellen, want hij sleepte zo'n zeven maanden geleden ook al een 'brief van de week' in de wacht. Gezien de populariteit van draadloos internetten, leek zijn probleem ons echter ook dit keer belangrijk genoeg voor vele andere Clickx-lezers: hoe beveilig en monitor ik mijn draadloze thuisnetwerk?



DRAADLOOS NETWERK BESCHERMEN



(DRAAD)LOOS ALARM!



WAT DOEN WE?

- JE DRAADLOZE THUISNETWERK BEVEILIGEN EN MONITOREN

WAARMEE?

- STANDAARDTECHNIEKEN EN EXTRA TOOLS ALS LOOK@LAN NETWERK MONITOR EN NETWORK MAGIX

HOELANG?

- CIRCA 1 UUR

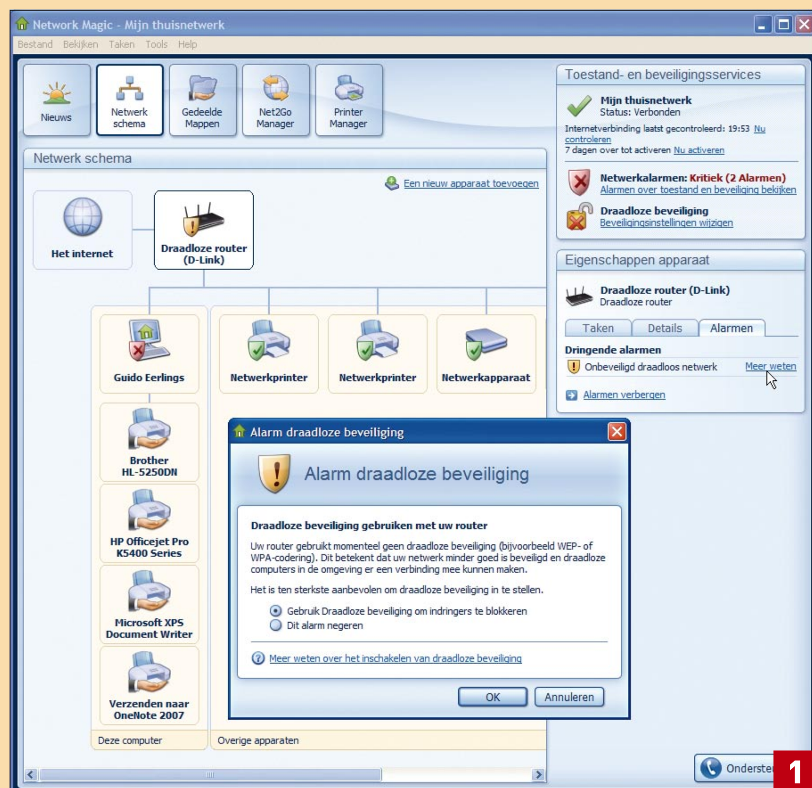
MOEILIJKHEID?



In Clickx hebben we het al enkele keren gehad over standaardtechnieken om een draadloos netwerk (WLAN of wireless LAN) te beveiligen: we vatten de belangrijkste methodes nog even samen in ons eerste kaderstukje. In het tweede kadertje vermelden we nog een paar extra tips en tools om je WLAN te 'monitoren'. In de eigenlijke workshop stellen we je in een notendop een tool met een veelbelovende naam voor: Network Magic (gratis in een afgeslankte versie; de premium-versie kost € 28,99 voor 3 pc's). De grootste verdienste van dit programma is dat het allerlei onderdelen van je netwerk overzichtelijk en vlot toegankelijk maakt. We houden het op deze pagina's echter bij het beveiligen en monitoren van ons WLAN.

STAP 1 / INSTALLATIE & BASISCONFIGURATIE

Surf naar www.networkmagic.eu en download (de Nederlandstalige versie van) de tool (5,89 MB). Dubbelklik op het uitvoerbare bestand en druk op **Volgende**. Verklaar je akkoord met de licentieovereenkomst en bevestig met **Volgende**. Kies een geschikte installatiemap uit en rond af met **Installeren** en **Voltooien**. Sus maar meteen je firewall, mocht die opschrikken: Network Magic is immers een betrouwbaar brokje software. Even later vraagt een wizard je dan om de login-id van je netwerkrouter. Geef gebruikersnaam en wachtwoord in: Network Magic moet die immers zelf kunnen 'bevragen' om zo een en ander te kunnen configureren en automatiseren. Bevestig met **Volgende** (driemaal). Vul je e-mailadres in om een tijdlang van de Premium-extraatjes te kunnen genieten: een overzicht hiervan vind je op de vermelde site. Zorg ook dat je firewall correct staat ingesteld (Network Magic biedt je hiervoor een link aan met stapsgewijze instructies). Sluit de wizard af met **Voltooien**. Oh ja, via support@networkmagic.eu kan je op enige ondersteuning rekenen (de 'helpdesk' op 016/27.07.57 blijkt niet echt veel soeps). Je belandt nu in het hoofdvenster van Network Magic (zie afbeelding 1).



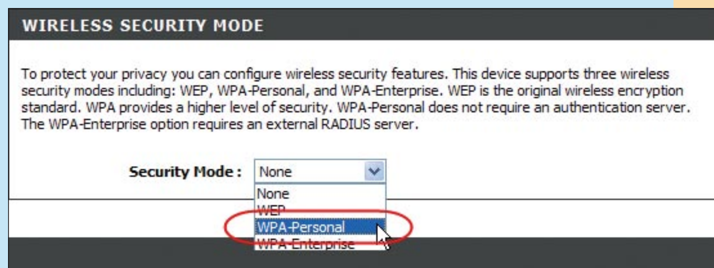
Veel netwerkinformatie aan je vingertoppen...

VERSLEUTELING: DE KORTSTE WEG NAAR EEN VEILIG WLAN

De meest trefzekere manier om je draadloos netwerkje tegen onbevoegde gebruikers af te schermen, is dataversleuteling. Deze encryptie moet je zowel op je draadloze router of toegangspunt als op de draadloze netwerkadapter(s) van je pc('s) instellen. Gewoonlijk bereik je het configuratievenster van je router of toegangspunt via een webinterface. Tik hiervoor het ip-adres van het toestel in je browser in. Dit adres lees je af bij **Gateway** als je de opdracht *ipconfig* uitvoert in een DOS-venster.

Oudere modellen bieden je mogelijk alleen WEP (Wired Equivalent Privacy) aan, maar deze standaard is al langer onveilig gebleken. Met wat geluk kan je via een update van de firmware toch nog het betere WPA activeren (WiFi Protected Access). Voor thuisgebruik wordt dat dan normaal gezien de variant WPA(2)-PSK met TKIP. Geef in elk geval een zo lang mogelijke, complexe sleutel in en vergeet die niet!

Als bijkomende maatregelen, die echter lang niet zo efficiënt zijn, vermelden we nog het uitschakelen van SSID Broadcast op je router of toegangspunt (zodat de netwerknaam niet wordt uitgezonden), het inschakelen van mac-filtering (zodat alleen pc's met een specifieke netwerkadapter je netwerk op kunnen) en het beveiligen van je router of toegangspunt met een stevig beheerderswachtwoord. Een Nederlandstalige handleiding met meer achtergrondinformatie en stapsgewijze instructies vind je op www.tekstenuitleg.net/artikelen/draadloos_netwerk_beveiligen/1.



WPA(2): de beste beveiliging voor je draadloze thuisnetwerkje!

NIET BINNEN ZONDER KLOPPEN!

Met een stevige WPA(2)-beveiliging kan je al rustig op je beide oren slapen. Weet je echter niet alle paranoia van je af te schudden, dan kan je nog op diverse manieren nagaan wie – of toch: welke pc – er wanneer op je WiFi-golven meesurft. Roep de web-interface van je router op (zie ander kaderstukje), meld je aan als beheerder en ga op zoek naar een rubriek als **Status**. Hier tref je ongetwijfeld een item aan als **Logs** en/of **Wireless**, en gewoonlijk lees je hier ook de ip-adressen af van de clients die zich op dat moment van je draadloze netwerkje bedienen.
De gratis tool Look@LAN Network Monitor (voor Windows XP) biedt je echter een iets meer geautomatiseerde manier aan. Dit programma wordt weliswaar al een tijdlang niet verder ontwikkeld, maar het is nog altijd perfect bruikbaar. Je kan het downloaden op www.lookatlan.com. Hoe je ervoor zorgt dat je automatisch een bericht of zelfs een e-mail krijgt zodra een (nieuwe) pc zich op het (draadloze) netwerk aanmeldt, lees je in de rubriek Top downloads, op pagina 62 in deze Clickx Magazine.

De meeste routers tonen je het ip- en mac-adres van de aangesloten toestellen.

STAP 2 / DRAADLOZE BEVEILIGING

In het centrale paneel vind je een handig overzicht van alle actieve toestellen in je netwerk. Rechtsboven merk je het paneel **Toestand- en beveiligingsservices** op. Klik hier op de link **Beveiligingsinstellingen wijzigen**, in de rubriek **Draadloze beveiliging**. In een nieuw venstertje verschijnen nu drie belangrijke opties: **Netwerkvergrendeling**, **Uitzending Netwerknaam** en **Codering** (zie afbeelding 2). Niks nieuws voor wie ons eerste kaderstukje heeft doorgenomen, maar makkelijk is wel dat je deze drie opties hier netjes onder elkaar krijgt opgedist. We raden je alvast aan (WPA-)codering in te schakelen; afhankelijk van het routertype kan je dat wellicht vanuit Network Magic regelen. Zoniet, dan moet je via de webinterface van je router werken (zie kaderstukjes). Netwerkvergrendeling is eigenlijk niks anders dan mac-adresfiltering: als je geen bijkomende toestellen op je netwerkje wil, kan je dit gerust activeren. En je maakt het potentiële indringers ook weer net dat tikkeltje lastiger als je ervoor zorgt dat de netwerknaam niet wordt uitgezonden.



Het 'gevarendriehoekje' is hier meer dan terecht!

STAP 3 / MONITORING

Met Network Magic kan je je netwerkje dus makkelijk afschermen, maar wat als een indringer toch een gaatje prikt? Dan laat je Network Magic aan de alarmbel trekken! Ga naar het menu **Tools** en kies **Opties**. Plaats zeker al een vinkje bij **Start Network Magic als Windows wordt gestart**, **Volg nieuwe apparaten automatisch als indringers**, [Geef een melding weer als...] **een nieuw apparaat aan het netwerk wordt toegevoegd**, en eventueel ook bij **een bekend apparaat opnieuw op het netwerk wordt aangesloten** (als je bijvoorbeeld wil weten wanneer zoonlief weer eens online gaat). Het is ook mogelijk om een al bekende pc als een indringer te laten beschouwen. Klik erop met de rechtermuisknop in het netwerkoverzicht en kies **Volgen als indringer**. Alle belangrijke meldingen kan je dan op elk moment bekijken via de link **Alarmen over toestand en beveiliging bekijken** (in het paneel rechtsboven) of door de knop **Nieuws** aan te klikken (zie afbeelding 3). Lees je hier bijvoorbeeld *1 indringer op het netwerk gedetecteerd*, dan hoef je hier maar op te klikken om in het eigenschappenpaneel meer informatie over deze indringer te verkrijgen (zoals mac- en ip-adres). Happy hunting! ♦



Alarm! Indringer gedetecteerd...